performing a randomization function over said plurality of hidden ciphertext blocks to create a plurality of output ciphertext blocks each of ℓ bits in length.

66. (New) The method as defined in claim 65,

wherein said making one and only one processing pass step comprises processing each of said equal-sized blocks and the MDC block by an encryption scheme that is confidentiality-secure against chosen-plaintext attacks, wherein each of said equal-sized blocks and the MDC block is processed by a block cipher using a first secret key to obtain said plurality of hidden ciphertext blocks; and

wherein said performing a randomization function step comprises combining each of said hidden ciphertext blocks with a corresponding element of a sequence of unpredictable elements to create a set of output blocks of the ciphertext, wherein a hidden ciphertext block identified by an index i is combined with the element of the sequence identified by index i by an operation that has an inverse.

67. (New) The method as defined in claim 65, wherein said generating a plurality of equal-sized blocks of ℓ bits in length from the input plaintext string further comprises the steps of:

padding the input plaintext string as necessary such that its length is a multiple of ℓ bits; and

partitioning the padded input plaintext string into a plurality of equal-size blocks of ℓ bits in length.

68. (New) The method as defined in claim 67, wherein said padding of the input plaintext string is a standard padding method.

69. (New) The method as defined in claim 66,

wherein the result of the combination of any two different unpredictable elements of the sequence of unpredictable elements by the inverse operation of the operation to create a set of output blocks of the ciphertext is unpredictable; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of the same sequence of unpredictable elements used for the encryption of said plaintext string; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of a plurality of sequences of unpredictable elements used for encryption of a plurality of plaintext strings with the same secret key K.

70. (New) The method as defined in claim 2,

wherein the result of the combination of any two different unpredictable elements of the sequence of unpredictable elements by the inverse operation of the operation to create a set of output blocks of the ciphertext is unpredictable; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of the same sequence of unpredictable elements used for the encryption of said plaintext string; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of a plurality of sequences of unpredictable elements used for encryption of a plurality of plaintext strings with the same secret key K.

71. (New) A program product for an encryption method for providing both data confidentiality and integrity for a message, including machine-readable code for causing a machine to perform the following method steps:

receiving an input plaintext string comprising a message;

generating a plurality of equal-sized blocks of ℓ bits in length from the input plaintext string;

creating an MDC block of ℓ bits in length that includes the result of applying a non-cryptographic Manipulation Detection Code (MDC) function to the plurality of the equal-sized blocks;

making one and only one processing pass with a single cryptographic primitive over each of said equal-sized blocks and the MDC block to create a plurality of hidden ciphertext blocks each of ℓ bits in length; and

performing a randomization function over said plurality of hidden ciphertext blocks to create a plurality of output ciphertext blocks each of ℓ bits in length.

72. (New) The program product defined in claim 71, wherein the program code for causing the performance of the step of making one and only one processing pass step comprises processing each of said equal-sized blocks and the MDC block by an encryption scheme that is confidentiality-secure against chosen-plaintext attacks,

wherein each of said equal-sized blocks and the MDC block is processed by a block cipher using a first secret key to obtain said plurality of hidden ciphertext blocks; and

wherein the program code for causing the performing a randomization function step comprises combining each of said hidden ciphertext blocks with a corresponding element of a sequence of unpredictable elements to create a set of output blocks of the ciphertext, wherein a hidden ciphertext block identified by an index i is combined with the element of the sequence identified by index i by an operation that has an inverse.

73. (New) The program product defined in claim 71, wherein the program code for performing said step of generating a plurality of equal-sized blocks of ℓ bits in length from the input plaintext string further comprises code for performing the steps of:

a' cont

padding the input plaintext string as necessary such that its length is a multiple of ℓ bits; and

partitioning the padded input plaintext string into a plurality of equal-size blocks of ℓ bits in length.

74. (New) The program product defined in claim 73,

wherein the program code for performing said step of padding of the input plaintext string comprises code for performing a standard padding method.

75. (New) The program product defined in claim 72,

wherein the result of the combination of any two different unpredictable elements of the sequence of unpredictable elements by the inverse operation of the operation to create a set of output blocks of the ciphertext is unpredictable; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of the same sequence of unpredictable elements used for the encryption of said plaintext string; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of a plurality of sequences of unpredictable elements used for encryption of a plurality of plaintext strings with the same secret key K.

76. (New) The program product defined in claim 48,

wherein the result of the combination of any two different unpredictable elements of the sequence of unpredictable elements by the inverse operation of the operation to create a set of output blocks of the ciphertext is unpredictable; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of the same sequence of unpredictable elements used for the encryption of said plaintext string; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of a plurality of sequences of unpredictable elements used for encryption of a plurality of plaintext strings with the same secret key K.

77. (New) An encryption system for providing both data confidentiality and integrity for a message, comprising:

a first component for receiving an input plaintext string comprising a message;

a second component for generating a plurality of equal-sized blocks of ℓ bits in length from the input plaintext string;

a third component for creating an MDC block of ℓ bits in length that includes the result of applying a non-cryptographic Manipulation Detection Code (MDC) function to the plurality of the equal-sized blocks;

a fourth component for making one and only one processing pass with a single cryptographic primitive over each of said equal-sized blocks and the MDC block to create a plurality of hidden ciphertext blocks each of ℓ bits in length; and

a fifth component for performing a randomization function over said plurality of hidden ciphertext blocks to create a plurality of output ciphertext blocks each of ℓ bits in length.

78. (New) The system as defined in claim 77,

wherein said fourth component for making one and only one processing pass comprises a component for processing each of said equal-size blocks and the MDC block by an encryption scheme that is confidentiality-secure against chosen-plaintext attacks, wherein each of said equal-sized blocks and the MDC block is processed by a block cipher using a first secret key to obtain said plurality of hidden ciphertext blocks; and

wherein fifth component for performing a randomization function comprises a component for combining each of said hidden ciphertext blocks with a corresponding

element of a sequence of unpredictable elements to create a set of output blocks of the ciphertext, wherein a hidden ciphertext block identified by an index i is combined with the element of the sequence identified by index i by an operation that has an inverse.

79. (New) The system as defined in claim 77, wherein said second component for generating a plurality of equal-sized blocks of ℓ bits in length from the input plaintext string further comprises components for

padding the input plaintext string as necessary such that its length is a multiple of ℓ bits; and

partitioning the padded input plaintext string into a plurality of equal-size blocks of ℓ bits in length.

80. (New) The system as defined in claim 79, wherein the said component for padding of the input plaintext string comprises a component for a standard padding method.

81. (New) The system as defined in claim 78,

wherein the result of the combination of any two different unpredictable elements of the sequence of unpredictable elements by the inverse operation of the operation to create a set of output blocks of the ciphertext is unpredictable; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of the same sequence of unpredictable elements used for the encryption of said plaintext string; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of a plurality of sequences of unpredictable elements used for encryption of a plurality of plaintext strings with the same secret key K.

82. (New) The system as defined in claim 53,

wherein the result of the combination of any two different unpredictable elements of the sequence of unpredictable elements by the inverse operation of the operation to create a set of output blocks of the ciphertext is unpredictable; and

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of the same sequence of unpredictable elements used for the encryption of said plaintext string; and

Q'
omit

wherein said unpredictable elements selected as said two unpredictable elements are any two different elements of a plurality of sequences of unpredictable elements used for encryption of a plurality of plaintext strings with the same secret key K.